



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,212	01/29/2002	Robert J. Lambert	00001-0420	2200
27871	7590	05/26/2006	EXAMINER	
BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA			ABRISHAMKAR, KAVEH	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 05/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,212	LAMBERT, ROBERT J.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 March 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 and 3-11 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1 and 3-11 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This communication is in reply to the amendment filed on March 16, 2006. Claims 1-6 were originally received for consideration. Per the received amendment, claim 2 is cancelled, and claims 7-11 are added. Claims 1, and 3-11 are currently being considered.

Response to Arguments

2. Applicant's arguments with respect to claims 1 and 3-11 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, and 3-11 are rejected under 35 U.S.C. 102(a) and 35 U.S.C. 102 (e) as being anticipated by Dworkin et al. (U.S. Patent No. 6,230,179).

Regarding claim 1, Dworkin discloses:

A method of adding elements of a finite field F_{2^m} , where m is less than a predetermined number n , said method comprising the steps of:

a) storing a first and a second element in a pair of registers, each of said pair of registers comprising said predetermined number of machine words (column 4 lines 4-13);

b) establishing an accumulator having said predetermined number of machine words (column 5 lines 1-10);

c) computing for each of said machine words in said accumulator the exclusive-or of the corresponding machine words representing each of said first and second elements (column 9 lines 13-19, column 10 lines 1-8) to obtain a representation of a result of the addition of said elements (column 5 lines 33-45), and, upon completion of said computation, performing modular reduction to reduce said result to a predetermined number of words (column 4 lines 29-34, column 10 lines 43-53).

Regarding claim 3, Dworkin discloses:

A finite field multiplier operable to multiply two elements of one of a plurality of finite fields, said finite fields being partitioned into subsets, said multiplier comprising:

a) a plurality of wordsized finite field multipliers, each suitable for multiplying elements of each finite field in a respective subset of said plurality of finite fields (column 4 lines 35-44)

b) a finite field reducer configured to perform reduction in said one finite field (column 4 lines 29-34, column 10 lines 43-53);

c) a processor configured to

i) operate the wordsized finite field multiplier suitable for use with said one finite field to obtain an intermediate product (column 4 lines 29-34, column 10 lines 43-53); and

ii) operate said finite field reducer on said intermediate product to obtain the product of the two elements (column 4 lines 29-34, column 10 lines 43-53).

Regarding claim 4, Dworkin discloses:

A method of performing a finite field operation on at least one element r , of a finite field, comprising the steps of:

a) representing each element as a number of machine words (column 4 lines 4-13);

b) performing a wordsized operation on said representations, said wordsized operation corresponding to said finite field operation (column 4 lines 35-44);

c) completing said wordsized operation on said representations to obtain a result (column 4 lines 29-34, column 10 lines 43-53); and

d) performing a modular reduction of said result to reduce said result to a predetermined number of words (column 4 lines 29-34, column 10 lines 43-53).

Regarding claim 5, Dworkin discloses:

A finite field engine for performing a finite field operation on at least one element of a finite field chosen from a set of finite fields, said set of finite fields being divided into subsets according to their word size, comprising:

a) a finite field operator for each of said subsets (column 4 lines 29-34, column 10 lines 43-53);

b) a finite field reducer for each of said finite fields (column 4 lines 29-34, column 10 lines 43-53);

c) a processor configured to choose the finite field operator corresponding to the subset containing said chosen finite field and the finite field reducer for said chosen finite field and apply the chosen finite field operator to said element to produce an intermediate result and apply the chosen finite field reducer to said intermediate result to obtain the result of said finite field operation (column 4 lines 29-34, column 10 lines 43-53).

Regarding claim 6, Dworkin discloses:

A cryptographic system comprising:

a) a plurality of elliptic curves, each specifying elliptic curve parameters and a respective finite field (column 1 lines 40-43), wherein the plurality of elliptic curves correspond to the different sized fields;

b) a plurality of finite field settings corresponding to each finite field (column 1 lines 40-45), wherein the finite fields can be of different sizes;

c) a plurality of wordsized finite fields, each having routines, each finite field being assigned to one of said wordsized finite fields (column 1 lines 40-45), wherein the finite fields can be of different sizes;

d) a reduction routine for each finite field (column 4 lines 29-34, column 10 lines 43-53);

e) a computational apparatus configured to perform a cryptographic operation by the steps of:

i) selecting one of said elliptic curves (paragraphs 18-22);

ii) performing a cryptographic function using the routines from the wordsized finite field to which the respective finite field corresponding to said selected elliptic curve is assigned (column 4 lines 35-44), said routines including at least one finite field operation and, subsequent thereto, a modular reduction to obtain a result of said operation corresponding to a predetermined number of words (column 4 lines 29-34, column 10 lines 43-53).

Claim 7 is rejected as applied above in rejecting claim 4. Furthermore, Dworkin:

Art Unit: 2131

A method according to claim 4 wherein said modular reduction is determined by said finite field (column 4 lines 29-34, column 10 lines 43-53).

Claim 8 is rejected as applied above in rejecting claim 4. Furthermore, Dworkin discloses:

A method according to claim 4 wherein said finite field operation is addition (column 5 lines 33-45).

Claim 9 is rejected as applied above in rejecting claim 4. Furthermore, Dworkin discloses:

A method according to claim 4 wherein said finite field operation is subtraction (column 10 lines 4-7, column 11 lines 5-11).

Claim 10 is rejected as applied above in rejecting claim 4. Furthermore, Dworkin discloses:

A method according to claim 4 wherein said finite field operation is multiplication (column 4 lines 35-44).

Claim 11 is rejected as applied above in rejecting claim 4. Furthermore, Dworkin discloses:

A method according to claim 4 wherein said finite field operation is division (column 5 lines 55-65).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
05/18/2006


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100